PATENT ABSTRACTS OF JAPAN

(11)Publication number : **09-282235**
(43)Date of publication of application : **31.10.1997**

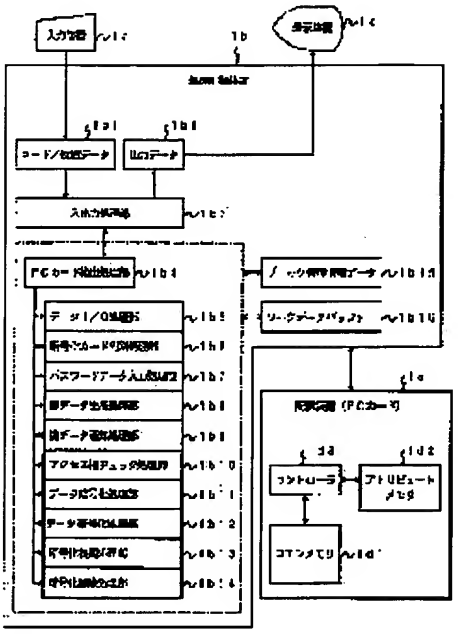
(51)Int.Cl. **G06F 12/14**
G06F 3/06
G06K 17/00

(21)Application number : **08-096900**
(22)Date of filing : **18.04.1996**

(71)Applicant : **TOSHIBA CORP**
(72)Inventor : **MIURA YOSHIYUKI**

(54) ACCESS CONTROL METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To improve the security of a portable storage medium such as a PC card.
SOLUTION: When a ciphering request for using a non-ciphered PC card 1d as a cipher card is issued from a user, the user is urged to input a password to be used in key data generation for the ciphering and deciphering processings of the PC card 1d. Then, the password inputted from the user is stored in the PC card 1d, key data are generated by utilizing the data and the key data are presented to the user. Thereafter, based on the generated key data, the ciphering processing of the data already stored in the mounted PC card 1d and the processing of re-storing the ciphered data in the PC card 1d are performed. Thus, the ciphering is performed even to the PC card 1d in use in which the data are already stored.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平9－282235

(43)公開日　平成９年(1997)10月31日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ　12/14	３２０		Ｇ０６Ｆ　12/14	３２０Ｂ	
3/06	３０４		3/06	３０４Ｈ	
Ｇ０６Ｋ　17/00			Ｇ０６Ｋ　17/00	Ｅ	

審査請求　未請求　請求項の数４　ＯＬ　（全 12 頁）

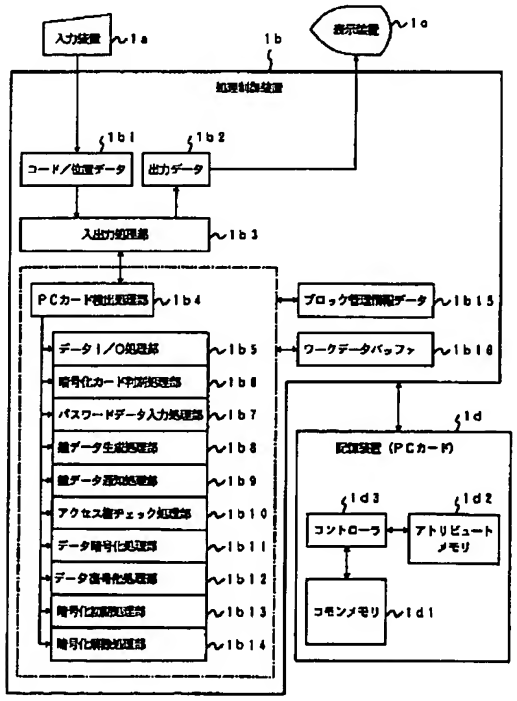
(21)出願番号　特願平8－96900

(22)出願日　平成８年(1996)４月18日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地
(72)発明者　三浦　佳之
東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内
(74)代理人　弁理士　鈴江　武彦　（外６名）

(54)【発明の名称】　アクセス制御方法

(57)【要約】
【課題】ＰＣカードなどの可搬型記憶媒体に対するセキュリティー性の向上を図る。
【解決手段】暗号化されてないＰＣカード１ｄを暗号カードとして使用する暗号化要求がユーザから発行されると、ＰＣカード１ｄの暗号化および復号化処理のためのキーデータ生成に用いるパスワードの入力がユーザに促される。そしてユーザから入力されたパスワードをＰＣカード１ｄに格納すると共に、そのデータを利用してキーデータを生成し、そのキーデータをユーザに提示する。この後、生成したキーデータに基づいて、装着されたＰＣカード１ｄに既に格納されているデータの暗号化処理、およびその暗号化データをＰＣカード１ｄに再格納する処理が行われ、これによって、既にデータが格納されている使用中のＰＣカード１ｄに対してもその暗号化が行われる。



1

【特許請求の範囲】

【請求項１】　可搬型記憶媒体が取り外し自在に装着される計算機システムで使用されるアクセス制御方法において、

前記計算機システムに装着された可搬型記憶媒体に対する暗号化要求に応じて、ユーザからの入力パスワードに基づいて前記可搬型記憶媒体に格納するデータを暗号化／復号化するためのキーデータを生成してそれをユーザに提示すると共に、前記入力パスワードを前記可搬型記憶媒体に格納し、

前記生成したキーデータに基づいて、前記装着された可搬型記憶媒体に既に格納されているデータを暗号化し、その暗号化データを前記可搬型記憶媒体に再格納し、

前記暗号化データを格納する可搬型記憶媒体が前記計算機システムに装着されたとき、前記可搬型記憶媒体から読み出した入力パスワードから暗号化／復号化用キーデータを生成し、その生成した暗号化／復号化用キーデータとユーザから入力される暗号化／復号化用キーデータとの比較結果に基づいて前記可搬型記憶媒体に対するアクセス権の有無を判定し、

アクセス権を有すると判定されたとき、前記可搬型記憶媒体に対するデータ書き込み／読み出し要求に応じて、ライトデータの暗号化およびその暗号化データの書き込み、または暗号化データの読み出しおよびその復号化を行うことを特徴とするアクセス制御方法。

【請求項２】　前記アクセス権を有すると判定されたとき、前記可搬型記憶媒体に対する暗号化解除要求に応じて、前記可搬型記憶媒体から前記入力パスワードを削除すると共に、前記暗号化されて格納されているデータを復号化して、前記可搬型記憶媒体に再格納することを特徴とする請求項１記載のアクセス制御方法。

【請求項３】　可搬型記憶媒体が取り外し自在に装着される計算機システムで使用されるアクセス制御方法において、

前記可搬型記憶媒体が前記計算機システムに装着されたとき、その装着された可搬型記憶媒体が暗号化媒体であるか否かを検出し、

前記装着された可搬型記憶媒体が非暗号化媒体であるとき、ユーザからの暗号化要求に応じて、入力パスワードに基づいて前記可搬型記憶媒体に格納するデータを暗号化／復号化するためのキーデータを生成してそれをユーザに提示すると共に、前記入力パスワードを前記可搬型記憶媒体に格納し、

前記生成したキーデータに基づいて、前記可搬型記憶媒体に既に格納されているデータを暗号化し、その暗号化データを前記可搬型記憶媒体に再格納し、

前記装着された可搬型記憶媒体が暗号化媒体であるとき、前記可搬型記憶媒体から読み出した入力パスワードから暗号化／復号化用キーデータを生成し、その生成した暗号化／復号化用キーデータとユーザから入力される

2

暗号化／復号化用キーデータとの比較結果に基づいて前記可搬型記憶媒体に対するアクセス権の有無を判定し、

アクセス権を有すると判定されたとき、前記可搬型記憶媒体に対するデータ書き込み／読み出し要求に応じて、ライトデータの暗号化およびその暗号化データの書き込み、または暗号化データの読み出しおよびその復号化を行うことを特徴とするアクセス制御方法。

【請求項４】　前記アクセス権を有すると判定されたとき、前記可搬型記憶媒体に対する暗号化解除要求に応じて、前記可搬型記憶媒体から前記入力パスワードを削除すると共に、前記暗号化されて格納されているデータを復号化して、前記可搬型記憶媒体に再格納することを特徴とする請求項３記載のアクセス制御方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、可搬型記憶媒体が取り外し自在に装着される計算機システムで使用されるアクセス制御方法に関する。

【０００２】

【従来の技術】従来、半導体メモリを内蔵したＰＣカードやフロッピーディスクなどの可搬型記憶媒体に対するデータ書き込みにおいては、書き込みデータを変形させることなく、そのままの状態で記憶媒体に格納するという方式が採用されており、データを書き込んだユーザ以外の他のユーザでも簡単にそのデータに対してアクセスすることができた。なお、この方式におけるデータセキュリティ方式としては、ハードウェア的にはライトプロテクトスイッチによる書き込み禁止や、ソフトウェア的にはファイルの属性情報を変更することによる書き込み禁止ファイルや隠しファイルなどが知られている。

【０００３】しかしながら、このようなセキュリティ方式を採用しても、ＰＣカード内やフロッピーディスクのデータ構成は誰でも容易に解析および確認することができ、かつ、それらの属性も容易に変更することができるため、十分な秘匿性を得ることはできなかった。

【０００４】また、セキュリティを考慮したデータの格納方式としては、ＰＣカードなどの記憶媒体内にパスワードデータを格納し、アクセス時にパスワード入力を行うことにより、その記憶媒体に格納されているパスワードとの照合を行い、アクセス権をチェックした後、データライトおよびリードを行う方式が知られている。さらに、記憶するファイルまたはディレクトリ毎に暗号化処理を行うことにより他のユーザがアクセスしても有効なデータを取得することができないようにする方式もある。なお、この時に使用される暗号化用のキー（鍵）データは、それぞれファイルまたはディレクトリの属性情報として付加され、これを取得することにより、暗号化後のデータの復号化が実現される。

【０００５】しかし、これらのセキュリティー方式においては、ＰＣカードなどの記憶媒体内にパスワードまた

は暗号化／復号化用キーデータ自体を格納しているため、Ｉ／Ｏアクセス時には解析できないものの、記憶媒体内のデータを解析することにより、それらの取得を行うことができ、その後容易にデータをアクセスすることができる。つまり、単一レベルでの秘匿しか行っていないため、容易にそれを解除することができ、これも秘匿性の低いものであった。

【０００６】

【発明が解決しようとする課題】上述したように、半導体メモリを内蔵したＰＣカードや、フロッピーディスクなどの可搬型記憶媒体に対する従来のセキュリティ方式では、第三者が容易に属性を変更することができたり、パスワードや暗号化用のデータを解析し取得することができるため、個人単位で携帯する可搬型記憶媒体の個人情報を秘匿化するセキュリティ技術としては信頼性の低いものであった。

【０００７】そこで、最近では、ファイルやディレクトリ単位ではなく、ＰＣカードなどの記憶媒体単位でそこに書き込むデータを暗号化するセキュリティー方式が本出願人により提案されている（特願平８－４２９１３号）。しかし、このセキュリティー方式は、ＰＣカードフォーマット時に、そのＰＣカードに今後書き込むライトデータに対して暗号化処理を行うための設定をＰＣカードに対して行う方式であるため、使用中のＰＣカードについては、それを再フォーマットしない限り暗号化処理を行うことはできない。このため、既にデータが格納されているＰＣカードに対しては、そのデータを格納したままの状態では、そのＰＣカードを暗号化処理することはできない。また、暗号化処理されたＰＣカードの秘匿を解除する機能が用意されておらず、解除するためには、ＰＣカードを再フォーマットしなければならないという問題があった。

【０００８】この発明はこの様な点に鑑みてなされたものであり、使用中の可搬型記憶媒体に対してもその媒体単位で秘匿性の高い暗号化処理を容易に行うことができるアクセス制御方法を提供することを目的とする。

【０００９】

【課題を解決するための手段】この発明は、可搬型記憶媒体が取り外し自在に装着される計算機システムで使用されるアクセス制御方法において、前記計算機システムに装着された可搬型記憶媒体に対する暗号化要求に応じて、ユーザからの入力パスワードに基づいて前記可搬型記憶媒体に格納するデータを暗号化／復号化するためのキーデータを生成してそれをユーザに提示すると共に、前記入力パスワードを前記可搬型記憶媒体に格納し、前記生成したキーデータに基づいて、前記装着された可搬型記憶媒体に既に格納されているデータを暗号化し、その暗号化データを前記可搬型記憶媒体に再格納し、前記暗号化データを格納する可搬型記憶媒体が前記計算機システムに装着されたとき、前記可搬型記憶媒体から読み出した入力パスワードから暗号化／復号化用キーデータを生成し、その生成した暗号化／復号化用キーデータとユーザから入力される暗号化／復号化用キーデータとの比較結果に基づいて前記可搬型記憶媒体に対するアクセス権の有無を判定し、アクセス権を有すると判定されたとき、前記可搬型記憶媒体に対するデータ書き込み／読み出し要求に応じて、ライトデータの暗号化およびその暗号化データの書き込み、または暗号化データの読み出しおよびその復号化を行うことを特徴とする。

【００１０】このアクセス制御方法によれば、ＰＣカードやフロッピーディスクなどの可搬型記憶媒体を暗号カードとして使用する暗号化要求がユーザから発行されると、可搬型記憶媒体の暗号化および復号化処理のためのキーデータ生成に用いるパスワードの入力がユーザに促される。そしてユーザから入力されたパスワードを可搬型記憶媒体に格納すると共に、そのデータを利用してキーデータを生成し、そのキーデータをユーザに提示する。このようにして、可搬型記憶媒体には、キーデータ生成に使用したパスワードだけが格納され、キーデータはアクセス制御方法を実現するためのＩ／Ｏ制御システムとして使用されるソフトウェア内部で保持管理される。この後、生成したキーデータに基づいて、装着された可搬型記憶媒体に既に格納されているデータの暗号化処理、およびその暗号化データを前記可搬型記憶媒体に再格納する処理が行われ、これによって、既にデータが格納されている使用中の可搬型記憶媒体に対してもその暗号化が行われる。

【００１１】暗号化された可搬型記憶媒体が計算機システムに装着されたときは、アクセス権チェックが行われる。このアクセス権チェックでは、ユーザにパスワードではなく、キーデータを入力させ、それが、可搬型記憶媒体から読み出したパスワードから生成したキーデータと比較される。そして、アクセス権を有すると判定された場合には、データ書き込み／読み出し要求に応じてライトデータの暗号化およびその暗号化データの書き込み、または暗号化データの読み出しおよびその復号化を行う。

【００１２】したがって、使用中の可搬型記憶媒体に対してもその媒体単位で秘匿性の高い暗号化処理を容易に行うことができる。また、記憶媒体には実際にデータ暗号化および復号化の際に使用されるキーデータを格納しておくのではなく、あくまでもそのキーデータを生成するための元となるパスワードのみが格納されているので、第三者が記憶媒体内のデータを単純に解析しただけでは秘匿を解くことはできない。よって、個人単位で携帯され、且つ計算機システムに着脱自在に装着して使用されるという特徴を持つ可搬型記憶媒体のセキュリティー保持に適したアクセス制御を実現できる。

【００１３】

【発明の実施の形態】以下、図面を参照してこの発明の

実施形態を説明する。図１には、この発明の一実施形態に係るアクセス制御方法が適用される計算機システムとそのシステムで実行されるプログラムの機能構成が示されている。ここでは、計算機システムに取り外し自在に装着可能な可搬型記憶媒体として、半導体メモリを搭載したＰＣカードを例にとって説明する。

【００１４】この計算機システムは、キーボードやマウスあるいはペンやトラックボールなどからなる入力装置１ａ、および表示装置１ｃを有する計算機本体を備えており、この計算機本体にはそれが電源オンの状態であってもＰＣカード１ｄの装着、取り外しを行うことができる。

【００１５】処理制御装置１ｂは、ＰＣカード１ｄの計算機システム本体との挿抜判別、ＰＣカード１ｄに対するデータ秘匿化の設定および設定解除、また、計算機システム本体からリクエストされたＩ／Ｏリクエストを判別し、データ暗号化および復号化処理を介してのＰＣカード１ｄへのデータＩ／Ｏ制御、また、これらの処理に応じた入力装置１ａおよび表示装置１ｃを介しての入出力制御を行うものであり、その機能は、計算機システム本体内のＣＰＵによって実行されるソフトウェアであるＰＣカードドライバを利用して実現されている。

【００１６】この処理制御装置１ｂは、入力装置１ａより入力されたコード／位置データ１ｂ１と表示装置１ｃに出力される文字データやグラフィックデータなどの出力データ１ｂ２を処理する入出力処理部１ｂ３と、計算機システム本体に対するＰＣカード１ｄの挿抜の検出、およびＰＣカードの種類の判別を行うＰＣカード検出処理部１ｂ４と、ＰＣカード１ｄに対するＩ／Ｏリクエストを判別し、ＰＣカード１ｄへのデータＩ／Ｏ処理を行うデータＩ／Ｏ処理部１ｂ５と、ＰＣカード検出処理部１ｂ４により検出、判別されたＰＣカードが暗号化されたＰＣカードであるか否かを判別する暗号化カード判別処理部１ｂ６と、暗号化されていないＰＣカード１ｄに対して暗号化／非暗号化の設定の選択および、暗号化する際の鍵データ（キーデータ）生成に使用するパスワードデータの入力およびＰＣカード１ｄへの格納を行うパスワード入力処理部１ｂ７と、パスワード入力処理１ｂ７により入力、格納されたパスワードデータより、データ暗号化／復号化用のキーデータ生成を行うキーデータ生成処理部１ｂ８と、キーデータ生成処理部１ｂ８により生成されたキーデータをユーザに通知するキーデータ通知処理部１ｂ９と、暗号化されているＰＣカード１ｄに対するアクセス権をチェックするためにキーデータの入力とそのデータの判別を行うアクセス権チェック処理部１ｂ１０と、暗号化されているＰＣカード１ｄに対してデータの書き込みを行う場合に、対象データを暗号化するデータ暗号化処理部１ｂ１１と、暗号化されているＰＣカード１ｄに対してデータの読み込みを行う場合に、対象データを復号化するデータ復号化処理部１ｂ１２と、計算機システム本体に正規のＰＣカード１ｄが装着され、そのＰＣカード１ｄに対して暗号化が設定された場合に、データＩ／Ｏ処理部１ｂ５とデータ暗号化処理部１ｂ１１により既にＰＣカード１ｄ内に格納されているデータの暗号化を行う暗号化初期処理部１ｂ１３と、計算機システム本体に正規のＰＣカード１ｄが装着され、ＰＣカード１ｄに対して暗号化の設定が解除された場合に、データＩ／Ｏ処理部１ｂ５とデータ復号処理部１ｂ１２により既にカード内に格納されているデータの復号化およびパスワードデータの削除を行う暗号化解除処理部１ｂ１４と、ＰＣカード内に格納するデータを管理するためのブロック管理情報データ１ｂ１５と、各処理部にて使用される変数の格納やバッファとして使用されるワークデータバッファ１ｂ１６とから構成される。

【００１７】また、ＰＣカード１ｄは、計算機システム本体からのデータＩ／Ｏコントロール処理信号に応じてコモンメモリ１ｄ１やアトリビュートメモリ１ｄ２へのデータリード／ライト制御を行うコントローラ１ｄ３と、このコントローラ１ｄ３を介して計算機システム本体から送信されるデータを格納するコモンメモリ１ｄ１と、ＰＣカード１ｄの属性情報が格納されているアトリビュートメモリ１ｄ２とにより構成される。なお、これらのメモリは、フラッシュＥＥＰＲＯＭなどの不揮発性メモリを使用して構成される。

【００１８】図２は、ブロック管理情報データ１ｂ１５の構成図である。ＰＣカードへ１ｄのデータライトは、ハードディスク装置やフロッピィディスク装置同様、ブロック（セクタ）単位でのデータＩ／Ｏ制御によって行われるため、ブロック管理情報データ１ｂ１５は、図示のように、ＰＣカード内の総ブロック数データ２ａと、使用不能となった不要ブロックを管理するための不良ブロック数データ２ｂと、不良ブロックとなったブロックＮｏ．１～Ｎデータ２ｃと、不良になったブロックの代替先であるスペアブロックのスペアブロック数データ２ｄと、スペアブロックの代替ブロック数であるスペアブロック登録数データ２ｅと、スペアブロックＮｏ．１～Ｎデータ２ｆを備えて構成する。

【００１９】図３は、アトリビュートメモリ１ｄ２の構成図である。アトリビュートメモリには、ＰＣカードサイズ３ａと、スペアブロック数３ｂと、製造メーカ名３ｃと、リリースバージョン３ｄと、パスワードデータ３ｄなどのカード属性情報が格納されている。

【００２０】以降、ＰＣカードドライバを利用して実行されるＰＣカード１ｄに対するアクセス制御の手順を説明する。まず、アクセス制御処理の基本的な流れについて説明する。

【００２１】ＰＣカード１ｄの装着時には、それが暗号化カードであるか否かが調べられ、暗号化カードでない場合には、ＰＣカード１ｄに対して暗号化処理を施すか

否かをユーザに選択させ、暗号化する場合に、その暗号化および復号化処理のための暗号化／復号化用キーデータを生成に用いるパスワードデータをユーザに入力させる。そして入力されたパスワードデータをＰＣカード１ｄ内に格納すると共に、そのデータを利用して暗号化／復号化用キーデータを生成し、そのキーデータをユーザにアナウンスする。そして、既に格納されているデータの暗号化、およびその暗号化データの再格納が行われる。装着されたカードが暗号化カードであった場合には、ユーザに暗号化／復号化用キーデータを入力させ、ＰＣカード１ｄへのアクセス権をチェックする。

【００２２】具体的には、以下のステップを利用してアクセス制御が行われる。

（１）ユーザに対して入力や確認を促す入出力ステップ。

（２）ＰＣカードと計算機システム本体との着脱状態や正規ＰＣカードの検出および判別を行うＰＣカード検出ステップ。

【００２３】（３）ＰＣカードに対するデータＩ／Ｏリクエストを判別し、リクエストに対応するデータＩ／Ｏ処理を行うデータＩ／Ｏステップ。

（４）カード内データより暗号化されているカードか否かをチェックし、その結果を入出力ステップによりユーザにアナウンスする暗号化カードチェックステップ。

【００２４】（５）暗号化カードチェックステップによりＰＣカードが暗号化されていないと判別された場合に、入出力ステップによりＰＣカードを暗号化するか否かの選択をユーザに促し、暗号化が選択された場合には暗号化／復号化用のキーデータの元となるデータの入力を促し、その結果ユーザが入力したデータをＰＣカード内に記憶するパスワード入力ステップ。

【００２５】（６）パスワード入力ステップにより入力し記憶されたパスワードデータを元に、実際にデータの暗号化／復号化時に使用される暗号化／復号化用のキーデータを生成するキーデータ生成ステップ。

【００２６】（７）キーデータ生成ステップにより生成されたキーデータを、入出力ステップによりユーザにアナウンスするキーデータ通知ステップ。

（８）暗号化カードチェックステップによりＰＣカードが暗号化されていると判別された場合に、入出力ステップによりデータ暗号化／復号化用のキーデータの入力をユーザに促し、そのデータがＰＣカード内に記憶されるパスワードデータを元にキーデータ生成ステップにより生成されたデータを比較することにより、ＰＣカードに対するアクセス権を判別するアクセス権チェックステップ。

【００２７】（９）アクセス権チェックステップによりＰＣカードに対するアクセス権を取得した場合のＰＣカードへのデータ書き込みに対して、キーデータ生成ステップによりデータ暗号化／復号化用キーデータを生成し、そのキーデータを元にデータを暗号化しＰＣカード内に格納するデータ暗号化ステップ。

【００２８】（１０）アクセス権チェックステップによりＰＣカードに対するアクセス権を取得した場合のＰＣカードのデータ読み出しに対して、キーデータ生成ステップによりデータ暗号化／復号化キーデータを生成し、そのキーデータを元にデータを復号化した結果をＩ／Ｏリクエストに渡すデータ復号化ステップ。

【００２９】（１１）暗号化カードチェックステップによりＰＣカードが暗号化されていないと判別された場合に、ＰＣカード内のデータの有無を判別し、パスワード入力ステップ、キーデータ生成ステップおよび、データ暗号化ステップにより、ＰＣカード内に格納されたパスワードデータを元にデータ暗号化／復号化用のキーデータを生成し、このキーデータを元にＰＣカード内のデータを暗号化する暗号化初期処理ステップ。

【００３０】（１２）暗号化カードチェックステップによりＰＣカードが暗号化されていると判別され、アクセス権チェックステップによりＰＣカードへのアクセス権を取得した場合に、入出力ステップによりＰＣカードの暗号化を解除するか否かの判別をユーザに促し、その結果ユーザが解除を選択した場合に、ＰＣカード内に格納されているパスワードデータを削除し、暗号化されたデータを復号化する暗号化解除ステップ。

【００３１】次に、図４のフローチャートを参照して、ＰＣカードアクセス制御処理におけるメイン処理の流れを説明する。ＰＣカード１ｄのアクセス制御は、計算機システム本体のメインメモリ（またはＥＭＳメモリ）に常駐するＰＣカードデバイスドライバによって実行されるものであり、このＰＣカードデバイスドライバは、計算機システム本体を起動した際にメインメモリ（またはＥＭＳメモリ）内への常駐や、ＰＣカードに対するＩ／Ｏポートアドレスの割り当て、あるいはＰＣカードスロットのディスクデバイスへの割り当てなどの初期化処理を行い、計算機システム本体に処理を戻す（ステップ４ａ～４ｃ）。これにより、ＰＣカードデバイスドライバは、割り当てられたディスクデバイスに対応するＰＣカードの装着待ち状態となる。

【００３２】計算機システム本体のＰＣカードスロットにＰＣカード１ｄが装着されると、計算機システム本体は、そのＰＣカード１ｄからのＰＣカード装着信号を検出し、ＰＣカードデバイスドライバをコールする。

【００３３】ＰＣカードデバイスドライバは、計算機システム本体からのアトリビュートメモリセレクト信号を受け取り、ＰＣカード検出処理部１ｂ４にて、ＰＣカード内のアトリビュートメモリ１ｄ２のデータをワークメモリデータバッファ１ｂ１６内に取り込み、装着されたＰＣカードが本デバイスドライバが認識可能なＰＣカードであるか否かを判別する（ステップ４ｄ、４ｅ）。

【００３４】この結果、本デバイスドライバが認識不可

能なＰＣカードと判別した場合は、入出力処理部１ｂ３を介して、ユーザに、正規でないまたはフォーマットされていないのＰＣカードであることをアナウンスし、計算機システム本体に処理を戻す（ステップ４ｆ～４ｈ）。

【００３５】また、本デバイスドライバが認識可能なＰＣカードと判別した場合は、暗号化カード判別処理部１ｂ６にて、取得したアトリビュートデータ内のパスワードデータ３ｅ領域内のデータをチェックし、暗号化処理が設定されているＰＣカードであるか否かを判別する（ステップ４ｉ）。この結果、暗号化処理が設定されていないＰＣカードと判別された場合、暗号化カード判別処理部１ｂ６は、入出力処理部１ｂ３を介してユーザに、暗号化されていないＰＣカードであることと、そのＰＣカードに暗号化処理を設定するか否かの選択をアナウンス表示する（ステップ４ｊ）。

【００３６】もしユーザが、暗号化設定を選択した場合には、ＰＣカード暗号化設定処理を行った後計算機システム本体に処理を戻し、設定しない方を選択した場合には、そのまま計算機システム本体に処理を戻す（ステップ４ｋ～４ｈ）。ＰＣカード暗号化設定処理の詳細は図５を参照して後述する。

【００３７】また、暗号化カード判別処理部１ｂ６にて既に暗号化処理が設定されているＰＣカードと判別された場合には、そのＰＣカードに対するアクセス権を取得するために、アクセス権チェック処理部１ｂ１０にて、入出力処理部１ｂ３を介してユーザに、暗号化処理が設定されたＰＣカードであることと、暗号化／復号化処理に使用されるキーデータの入力を促す（ステップ４ｏ）。そして、アトリビュートメモリより取得したデータ内のパスワードデータを元に生成したキーデータと、ユーザが入力したキーデータを比較する（ステップ４ｐ）。その結果、両者のキーデータが一致しない場合には、入出力処理部１ｂ３を介して、アクセス権が所得できないことをエラーとして表示した後、処理を計算機システム本体に戻す（ステップ４ｑ～４ｓ）。また、両者のキーデータが一致した場合には、入出力処理部１ｂ３を介してユーザに、暗号化処理が設定されたＰＣカードであることと、そのＰＣカードの暗号化処理設定を解除するか否かの選択をアナウンス表示する（ステップ４ｔ）。

【００３８】もしユーザが暗号化設定の解除を選択した場合には、ＰＣカード暗号化設定解除処理を行った後計算機システム本体に処理を戻し、設定解除しない方を選択した場合には、そのまま計算機システムに処理を戻す（ステップ４ｕ～４ｘ）。ＰＣカード暗号化設定解除処理の詳細は、図６を参照して後述する。

【００３９】また、計算機システム本体の入力装置よりＰＣカードに対応するディスクデバイスに対して、データライトあるいはデータリードなどのＩ／Ｏリクエストコマンドが入力された場合、データＩ／Ｏ処理にてＰＣカードの確認とデータＩ／Ｏ処理を行い、ステータス値をセットした後、計算機システム本体のデータＩ／Ｏコマンドに処理を戻す（ステップ４ｙ～４ａ′）。データＩ／Ｏ処理の詳細は、図７のフローチャートを参照して後述する。

【００４０】次に、上述したＰＣカード暗号化設定処理、ＰＣカード暗号化設定解除処理およびデータＩ／Ｏ処理の流れについて説明する。

（ＰＣカード暗号化設定処理）まず、ＰＣカード暗号化設定処理を図５のフローチャートを参照して説明する。

【００４１】本デバイスドライバのメイン処理より本処理がコールされると、パスワード入力処理部１ｂ７にて、入出力処理部１ｂ３を介してユーザにデータ暗号化／復号化処理に使用されるキーデータを生成するためのパスワードデータの入力を促す（ステップ５ａ）。ここで入力されたパスワードデータは、ＰＣカード内のアトリビュートメモリ１ｄ２内のパスワードデータ３ｅ領域に格納される（ステップ５ｂ）。

【００４２】そして、このパスワードデータを元に、キーデータ生成処理部１ｂ８にて、実際にデータ暗号化／復号化で使用されるキーデータを生成し、キーデータ通知処理部１ｂ９にて、ユーザに生成されたキーデータをアナウンスする（ステップ５ｃ、５ｄ）。

【００４３】また、ＰＣカード内の既に格納されているデータに対しても暗号化を行うため、暗号化初期処理部１ｂ１３にて、ＰＣカード内のブロック管理情報データを取得し、その情報に基づいてＰＣカード内のデータを取得し、データＩ／Ｏ処理部１ｂ５内の暗号化処理を経由したデータライト処理を介してデータを暗号化して、その暗号化データを同一格納位置に再度格納した後、メイン処理に処理を戻す（ステップ５ｅ～５ｇ）。

【００４４】（ＰＣカード暗号化設定解除処理）次に、ＰＣカード暗号化設定解除処理を図６のフローチャートを参照して説明する。

【００４５】本デバイスドライバのメイン処理より本処理がコールされると、暗号化解除処理部１ｂ１４にて、ＰＣカード内の前記アトリビュートメモリ１ｄ２データ内のパスワードデータ３ｅ領域内のデータを削除する（ステップ６ａ）。なお、この時点でＰＣカード内に格納されていたパスワードデータは削除するが、本処理がコールされる前にメイン処理で取得したキーデータはメモリ内に保持される。

【００４６】そして、ＰＣカード内に既に格納されているデータに対しても暗号化を解除するために、ＰＣカード内のブロック管理情報データを取得し、その情報とキーデータに基づいて、データＩ／Ｏ処理部１ｂ５内の復号化処理を経由したデータリード処理を介して暗号化されたデータを元に戻した後、暗号化処理を経由しないデータライト処理を介して、再度データを同一位置に格納

する（ステップ6ｂ～6ｃ）。以上の処理を行った後、処理をメイン処理に戻す（ステップ6ｄ）。

データＩ／Ｏ処理

（データＩ／Ｏ処理）次に、前述のデータＩ／Ｏ処理を図7のフローチャートを参照して説明する。なお、ここではデータＩ／Ｏ処理のうち、本発明に直接関係するデータライトおよびデータリード処理についてのみ説明する。

【００４７】本デバイスドライバのメイン処理または、ＰＣカード暗号化設定処理やＰＣカード暗号化設定解除処理より本処理がコールされると、データＩ／Ｏ処理部１ｂ5にて、ＰＣカードがデータＩ／Ｏ処理が可能な状態であるかを再度ＰＣカード内のアトリビュートメモリ内のデータを取得して確認する（ステップ7ａ）。その結果、ＰＣカードが認識可能なカードでなかったり、未装着であった場合には、入出力処理部１ｂ３を介してその旨をユーザにアナウンスし、処理をメイン処理に戻す（ステップ7ｂ、7ｃ）。

【００４８】ＰＣカードがデータＩ／Ｏ処理可能状態であった場合には、コール時に受け取ったデータＩ／Ｏリクエストの内容より、各処理に分岐して処理が行われる。データＩ／Ｏリクエストがデータライトである場合、ＰＣカード内のアトリビュートメモリ１ｄ２内のパスワードデータ３ｅまたはメモリ内にキーデータが存在するかを判別し、存在する場合にはキーデータを使用してデータを暗号化し（存在しない場合には直接）、コントローラ１ｄ３、アトリビュートメモリ内データおよびブロック管理情報データを介してコモンメモリ１ｄ１にデータを格納し、ステータス値をセットした後、メイン処理に処理を戻す（ステップ7ｄ～7ｈ）。

【００４９】また、データＩ／Ｏリクエストがデータリードである場合は、コントローラ１ｄ３、アトリビュートメモリ内データおよびブロック管理情報データを介してコモンメモリ１ｄ１のデータを取得し、ＰＣカード内のアトリビュートメモリ１ｄ２内のパスワード３ｅまたはメモリ内にキーデータが存在するかを判別し、存在する場合にはキーデータを使用してデータを復号化（存在しない場合には直接）し、ステータス値をセットした後、メイン処理に処理を戻す（ステップ7ｌ～7ｍ）。

【００５０】以上のように、この実施形態においては、ＰＣカード１ｄを暗号カードとして使用する暗号化要求がユーザから発行されると、ＰＣカード１ｄの暗号化および復号化処理のためのキーデータ生成に用いるパスワードの入力がユーザに促される。そしてユーザから入力されたパスワードをＰＣカード１ｄに格納すると共に、そのデータを利用してキーデータを生成し、そのキーデータをユーザに提示する。このようにして、ＰＣカード１ｄには、キーデータ生成に使用したパスワードだけが格納され、キーデータはデバイスドライバ内部で保持管理される。この後、生成したキーデータに基づいて、装着されたＰＣカード１ｄに既に格納されているデータの暗号化処理、およびその暗号化データをＰＣカード１ｄに再格納する処理が行われ、これによって、既にデータが格納されている使用中のＰＣカード１ｄに対してもその暗号化が行われる。

【００５１】また、暗号化されたＰＣカード１ｄが計算機システムに装着されたときは、アクセス権チェックが行われる。このアクセス権チェックでは、ユーザにパスワードではなく、キーデータを入力させ、それが、ＰＣカード１ｄから読み出したパスワードから生成したキーデータと比較される。そして、アクセス権を有すると判定された場合には、データ書き込み／読み出し要求に応じてライトデータの暗号化およびその暗号化データの書き込み、または暗号化データの読み出しおよびその復号化を行う。したがって、使用中のＰＣカード１ｄに対してもその媒体単位で秘匿性の高い暗号化処理を容易に行うことができる。

【００５２】また、記憶媒体には実際にデータ暗号化および復号化の際に使用されるキーデータを格納しておくのではなく、あくまでもそのキーデータを生成するための元となるパスワードのみが格納されているので、第三者が記憶媒体内のデータを単純に解析しただけでは秘匿を解くことはできない。よって、個人単位で携帯され、且つ計算機システムに着脱自在に装着して使用されるという特徴を持つ可搬型記憶媒体のセキュリティー保持に適したアクセス制御を実現できる。

【００５３】なお、ユーザに対するＰＣカードへの秘匿（暗号）化設定についての選択や、パスワードあるいは暗号化／復号化キーデータの入力を促す際のアナウンス手段として、本実施形態では計算機システム本体の表示装置を使用するように述べたが、図示しない計算機システム本体の音声出力装置により行う音声でのアナウンスなどであっても良い。また、表示形態としては、ＧＵＩを考慮したものであっても良い。また、データの暗号化および復号化処理として、本実施形態では具体的にその方式について述べなかったが、この方式については秘密鍵暗号方式や公開鍵暗号方式であっても良い。また、アクセス権をチェックする際に、キーデータが一致するまでのリトライ回数を複数回設けても良い。さらに、ＰＣカード内に格納されるパスワードデータについて、本実施形態では、ＰＣカード内のアトリビュートメモリ内に格納するように述べたが、コモンメモリ内であっても良い。暗号化するデータについてもＰＣカード全体であっても良いし、ディレクトリやファイル単位で行っても良い。

【００５４】また、本発明のデータの秘匿（暗号）化設定および秘匿化設定解除によるデータＩ／Ｏ制御方法については、ＰＣカードのみでなく、シリコンディスクやミニディスク、ＤＶＤなどの可搬型記憶媒体全てに応用可能な技術である。特に、秘匿化の設定および設定解除

13

を記憶媒体の計算機システム本体への装着時に行うようにすることにより、ユーザに負担をかけることなく行うことができるため、今後、個人情報のセキュリティが強化する傾向にある事から、本発明は有効である。

【００５５】

【発明の効果】以上説明したように、この発明によれば、ＰＣカードなどの可搬型記憶媒体に既に格納されているデータを暗号化して再格納する処理を具備することにより、使用中の可搬型記憶媒体に対しても暗号化の設定が可能となり、様々な小型携帯機器で使用され、今後益々個人レベルでの使用頻度が増加するＰＣカードなどの秘匿性を向上させることができる。また、可搬型記憶媒体の計算機システム本体への装着時に暗号化されたカードであるか否かを判別し、暗号化されたカードの場合はアクセス権チェック処理を行うことにより、ディレクトリやファイル単位でなくカード単位でのデータの暗号化を実現し、ユーザの操作に負担をかけることなくすることができる。さらに、暗号化解除処理を新たに追加したことにより、データ処理本体に可搬型記憶媒体を装着し、その記憶媒体に対するアクセス権チェックステップにてアクセス権を取得した時点で、暗号化されたＰＣカードを通常の状態に戻すことを実現することができる。

【図面の簡単な説明】

【図１】この発明の一実施形態に係るアクセス制御方法

14

が適用される計算機システムの構成を示すブロック図。

【図２】同実施形態の計算機システムで使用されるＰＣカードのデータ管理構造を説明するための図。

【図３】同実施形態の計算機システムで使用されるＰＣカードのアトリビュートメモリのデータ構造を説明するための図。

【図４】同実施形態の計算機システムにおけるアクセス制御処理の流れを説明するフローチャート。

【図５】同実施形態の計算機システムにおけるＰＣカード暗号化設定処理の流れを説明するフローチャート。

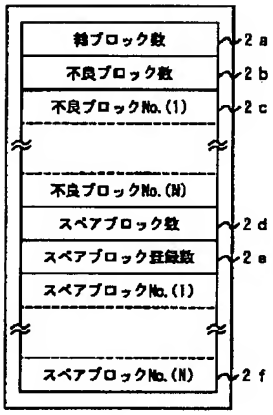
【図６】同実施形態の計算機システムにおけるＰＣカード暗号化設定解除処理の流れを説明するフローチャート。

【図７】同実施形態の計算機システムにおけるデータＩ／Ｏ処理の流れを説明するフローチャート。

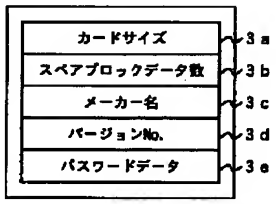
【符号の説明】

１ｂ…処理制御装置、１ｄ…ＰＣカード、１ｂ４…ＰＣカード検出処理部、１ｂ５…データＩ／Ｏ処理部、１ｂ６…暗号化カード判別処理部、１ｂ７…パスワードデータ入力処理部、１ｂ８…鍵データ生成処理部、１ｂ９…鍵データ通知処理部、１ｂ１０…アクセス権チェック処理部、１ｂ１１…データ暗号化処理部、１ｂ１２…データ復号化処理部、１ｂ１３…暗号化初期処理部、１ｂ１４…暗号化解除処理部。

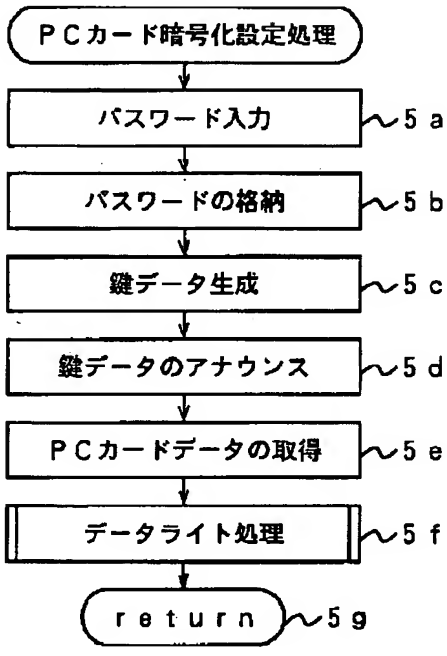
【図２】



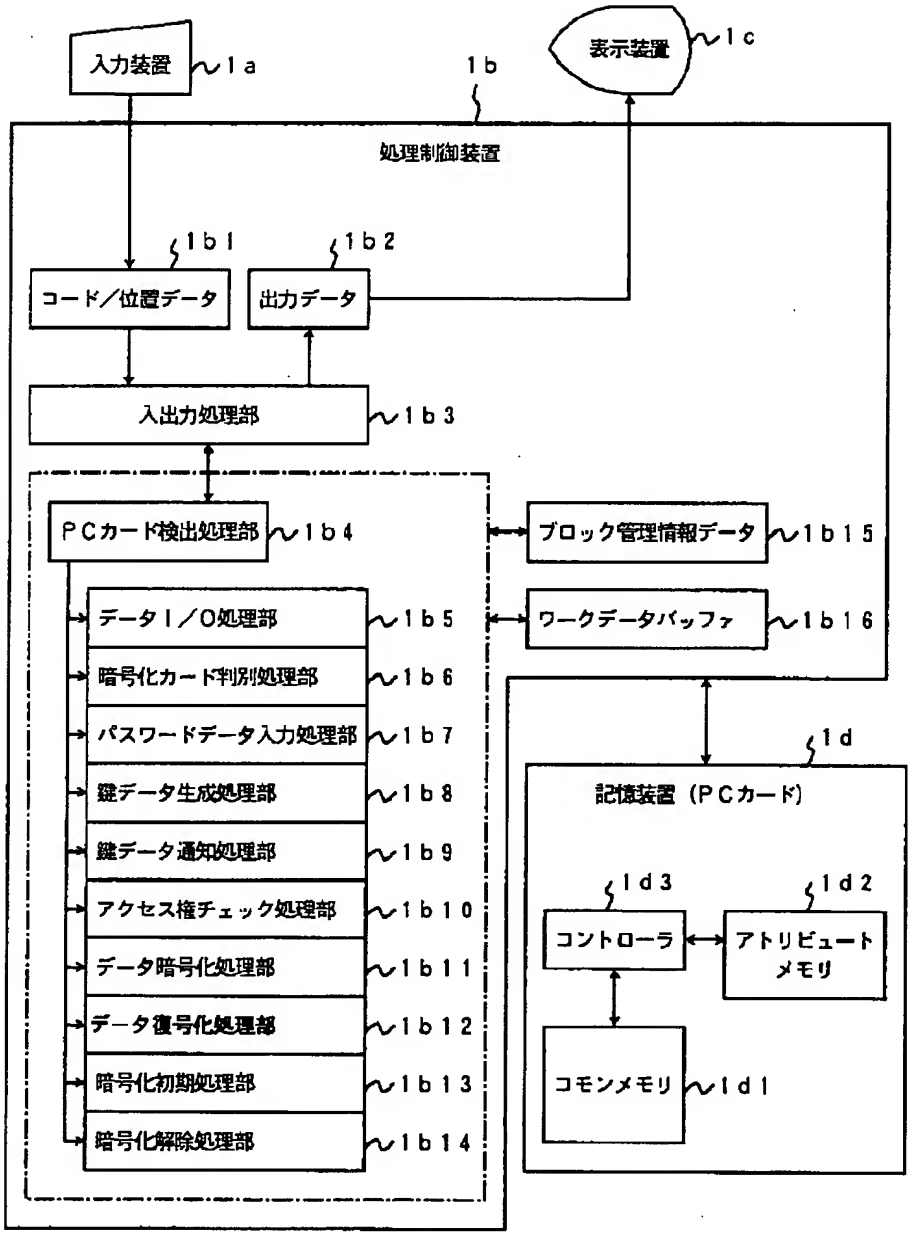
【図３】



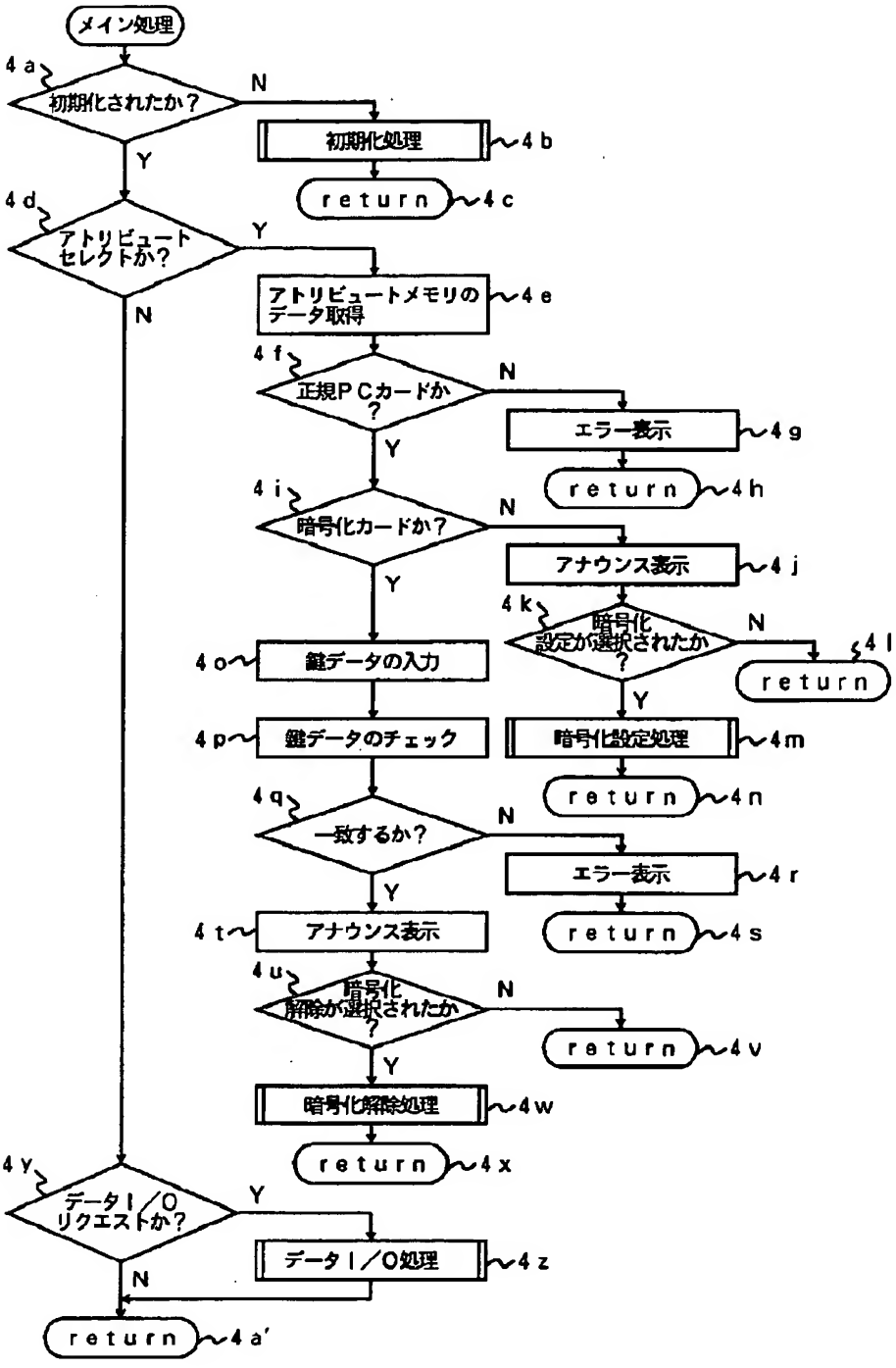
【図５】



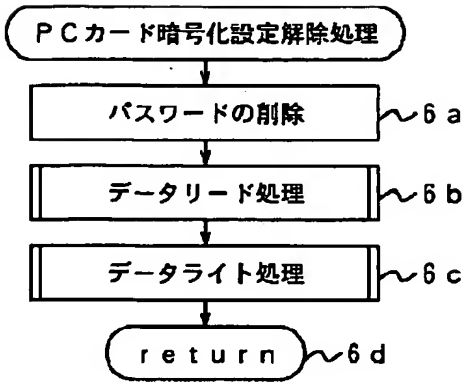
【図１】


入力装置
１ａ
１ｂ
表示装置
１ｃ
処理制御装置
１ｂ１
１ｂ２
コード／位置データ
出力データ
入出力処理部
１ｂ３
ＰＣカード検出処理部
１ｂ４
ブロック管理情報データ
１ｂ１５
データＩ／Ｏ処理部
１ｂ５
ワークデータバッファ
１ｂ１６
暗号化カード判別処理部
１ｂ６
パスワードデータ入力処理部
１ｂ７
鍵データ生成処理部
１ｂ８
鍵データ通知処理部
１ｂ９
アクセス権チェック処理部
１ｂ１０
データ暗号化処理部
１ｂ１１
データ復号化処理部
１ｂ１２
暗号化初期処理部
１ｂ１３
暗号化解除処理部
１ｂ１４
１ｄ
記憶装置（ＰＣカード）
１ｄ３
１ｄ２
コントローラ
アトリビュートメモリ
コモンメモリ
１ｄ１

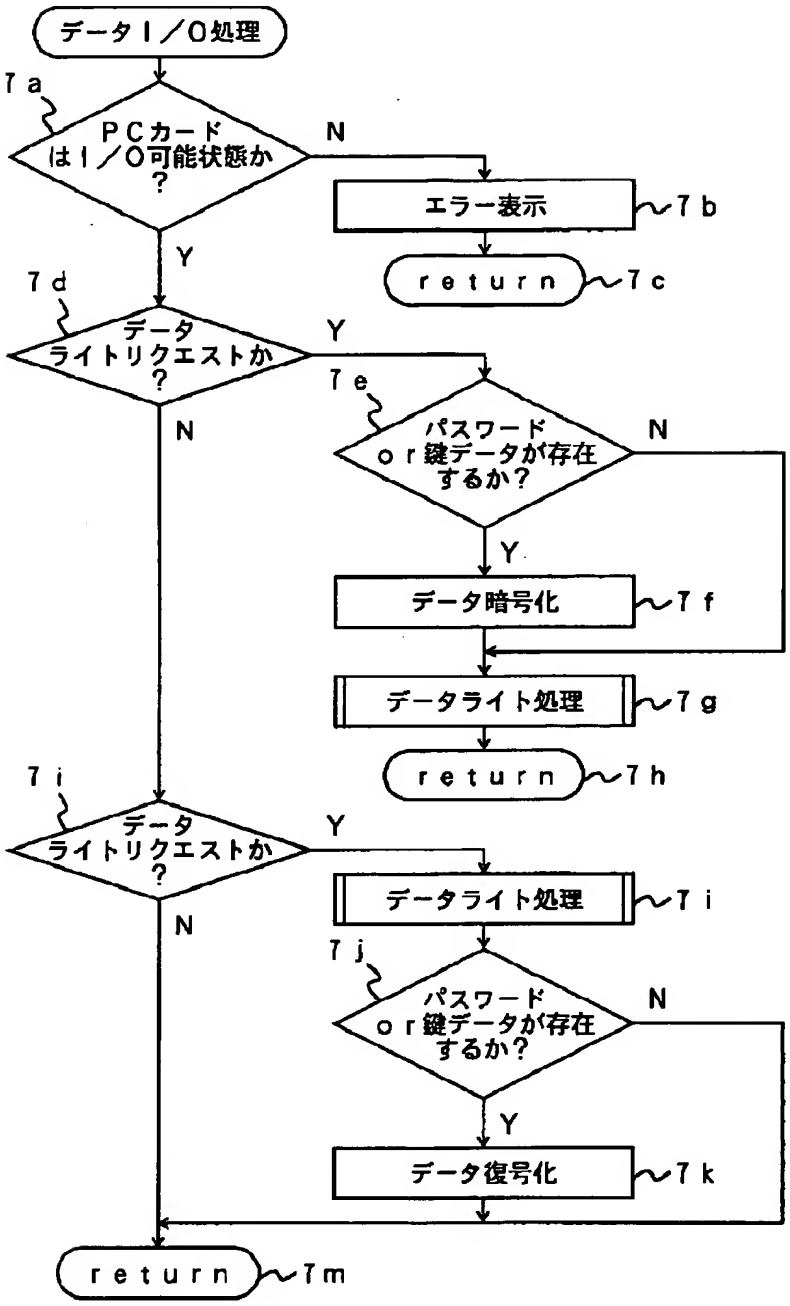
【図４】


メイン処理
4a
初期化されたか？
N
初期化処理
4b
return
4c
Y
4d
アトリビュート
セレクトか？
Y
アトリビュートメモリの
データ取得
4e
N
4f
正規ＰＣカードか
？
N
エラー表示
4g
return
4h
Y
4i
暗号化カードか？
N
アナウンス表示
4j
Y
4k
暗号化
設定が選択されたか
？
N
4l
return
Y
4o
鍵データの入力
4p
鍵データのチェック
暗号化設定処理
4m
return
4n
4q
一致するか？
N
エラー表示
4r
Y
4t
アナウンス表示
return
4s
4u
暗号化
解除が選択されたか
？
N
return
4v
Y
暗号化解除処理
4w
return
4x
4y
データＩ／Ｏ
リクエストか？
Y
データＩ／Ｏ処理
4z
N
return
4a'

【図６】


ＰＣカード暗号化設定解除処理
パスワードの削除
６ａ
データリード処理
６ｂ
データライト処理
６ｃ
ｒｅｔｕｒｎ
６ｄ

【図７】


データＩ／Ｏ処理
７ａ
ＰＣカード
はＩ／Ｏ可能状態か
？
N
エラー表示
７ｂ
Ｙ
ｒｅｔｕｒｎ
７ｃ
７ｄ
データ
ライトリクエストか
？
Y
７ｅ
パスワード
ｏｒ鍵データが存在
するか？
N
Y
データ暗号化
７ｆ
データライト処理
７ｇ
ｒｅｔｕｒｎ
７ｈ
７ｉ
データ
ライトリクエストか
？
Y
N
データライト処理
７ｉ
７ｊ
パスワード
ｏｒ鍵データが存在
するか？
N
Y
データ復号化
７ｋ
ｒｅｔｕｒｎ
７ｍ